

Sonus Networks, Inc.

SBC 5400 Session Border Controller

Firmware Version: R6.2.2

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1

Document Version: 0.8

Prepared for:



Sonus Networks, Inc.
4 Technology Park Drive
Westford, MA 01886
United States of America

Phone: +1 855 GO SONUS
www.sonus.net

Prepared by:



Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

- 1. Introduction4**
 - 1.1 Purpose4
 - 1.2 References4
 - 1.3 Document Organization4
- 2. SBC 5400 Session Border Controller5**
 - 2.1 Overview5
 - 2.2 Module Specification8
 - 2.3 Module Ports and Interfaces 11
 - 2.3.1 Front Bezel Interfaces 11
 - 2.3.2 Front Panel Interfaces 13
 - 2.3.3 Rear Panel Interfaces 13
 - 2.4 Roles, Services, and Authentication..... 15
 - 2.4.1 Authorized Roles 15
 - 2.4.2 Operator Services 16
 - 2.4.3 Additional Services 19
 - 2.4.4 Authentication 19
 - 2.5 Physical Security..... 21
 - 2.6 Operational Environment 21
 - 2.7 Cryptographic Key Management 21
 - 2.8 EMI / EMC 29
 - 2.9 Self-Tests 29
 - 2.9.1 Power-Up Self-Tests 29
 - 2.9.2 Conditional Self-Tests 30
 - 2.9.3 Critical Functions Self-Tests 30
 - 2.9.4 Self-Test Failure Handling 30
 - 2.10 Mitigation of Other Attacks 31
- 3. Secure Operation32**
 - 3.1 Initial Setup 32
 - 3.1.1 Hardware Installation and Commissioning 32
 - 3.1.2 Application Installation and Configuration 32
 - 3.1.3 Enabling FIPS-Approved Mode..... 33
 - 3.1.4 Restoring Service to EMA 34
 - 3.2 Crypto Officer Guidance 35
 - 3.2.1 Management 35
 - 3.2.2 Default CO Password Use..... 35
 - 3.2.3 On-Demand Self-Tests..... 35
 - 3.2.4 Zeroization..... 35
 - 3.2.5 Status Monitoring..... 36
 - 3.2.6 Firmware Upgrades 36
 - 3.3 User Guidance 37
 - 3.4 Additional Guidance and Usage Policies..... 37
 - 3.5 Non-Approved Mode of Operation 38

3.5.1	Security Functions	38
3.5.2	Roles	38
3.5.3	Services.....	38
4.	Acronyms	40

List of Tables

Table 1 – Security Level per FIPS 140-2 Section	7
Table 2 – FIPS-Approved Algorithm Implementations	8
Table 3 – Allowed Algorithms.....	10
Table 4 – FIPS 140-2 Logical Interface Mappings (Front Bezel).....	12
Table 5 – FIPS 140-2 Logical Interface Mappings (Front Panel)	13
Table 6 – FIPS 140-2 Logical Interface Mappings (Rear Panel)	14
Table 7 – Authorized Operator Services.....	16
Table 8 – Additional Services.....	19
Table 9 – Authentication Mechanism Used by the Module.....	20
Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs.....	22
Table 11 – Non-Approved Service	39
Table 12 – Acronyms	40

List of Figures

Figure 1 – Front View of SBC 5400	5
Figure 2 – A Typical Deployment Scenario of SBC 5400.....	7
Figure 3 – LEDs and Ports/Interfaces (Front Bezel).....	12
Figure 4 – LEDs and Ports/Interfaces (Front Panel).....	13
Figure 5 – LEDs and Ports/Interfaces (Rear Panel).....	14

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SBC 5400 Session Border Controller from Sonus Networks, Inc. (Sonus). This Security Policy describes how the SBC 5400 Session Border Controller meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The SBC 5400 Session Border Controller is referred to in this document as the SBC 5400 or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Sonus website (www.sonus.net) contains information on the full line of products from Sonus.
- The search page on the CMVP website (<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search>) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Sonus. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Sonus and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Sonus.

2. SBC 5400 Session Border Controller

2.1 Overview

Sonus Networks, Inc. (hereafter referred to as Sonus) is a leader in IP¹ networking with proven expertise in delivering secure, reliable and scalable next-generation infrastructure and subscriber solutions. The Sonus line of Session Border Controllers (SBC 5400) help mid-sized and large enterprises take advantage of cost-saving SIP² trunking services by securing their network from IP-based attacks, unifying SIP-based communications and controlling traffic in the network.

Sonus's SBC 5400 features a unique architecture design that differs from other session border controllers on the market today by aggregating all of the session border functionality – security, encryption, transcoding, call routing, and session management – into a single device and distributing those functions to embedded and modular hardware within the device. For example, media transcoding on the SBC 5400 is performed on a modular DSP³ farm, while much of the encryption is handled via embedded cryptographic hardware, thereby providing optimal performance during real-world workloads, overloads, and attacks.

The SBC 5400 Session Border Controller (see Figure 1 below) is a high-performance air-cooled, 2U, IP encryption appliance that provides secure SIP-based communications with robust security, reduced latency, real-time encryption (VOIP⁴ signaling and media traffic), media transcoding, flexible SIP session routing, and policy management.



Figure 1 – Front View of SBC 5400

The SBC 5400 is designed to fully address the next-generation need of SIP communications by delivering embedded media transcoding, robust security and advanced call routing in a high-performance, medium form-factor device. The SBC 5400 is designed to accommodate up to 75,000 call sessions. Some of the network and security features provided by the module include:

¹ IP – Internet Protocol

² SIP – Session Initiation Protocol

³ DSP – Digital Signal Processor

⁴ VOIP – Voice Over Internet Protocol

- Session-aware firewall, split DMZ⁵, bandwidth & QoS⁶ theft protection, topology hiding, DoS⁷/DDoS⁸ detection/blocking, rogue RTP⁹ protection, IPsec¹⁰ and TLS¹¹ encryption
- Embedded media transcoding hardware
- H.323 and SIP-I/T interworking
- Stateful call-handling even during overload/attack/outages
- Embedded localized or centralized call-routing options
- Far-end NAT¹² traversal
- TLS, IPsec (IKEv1¹³) for signaling encryption
- Secure RTP/RTCP¹⁴ for media encryption
- Support for large number of protocols including IPv4, IPv6, IPv4/IPv6 interworking, SSH¹⁵, SFTP¹⁶, SNMP¹⁷, HTTPS¹⁸, RTP/RTCP, UDP¹⁹, TCP²⁰, DNS²¹, and ENUM²²
- Exceptional scalability even under heavy workloads
- Device management using encrypted and authenticated device management messages
- Controlled menu access and comprehensive audit logs
- Integrated Baseband Management Controller (BMC)

The validated module is a solution that delivers end-to-end SIP session control and a networkwide view of SIP traffic and policy management. The module can be deployed as a peering SBC, access SBC, or enterprise SBC.

Figure 2 below illustrates a typical deployment scenario of the SBC 5400.

⁵ DMZ – Demilitarized Zone

⁶ QoS – Quality of Service

⁷ DoS – Denial of Service

⁸ DoS/DDoS – Denial-of-Service/Distributed Denial-of-Service

⁹ RTP – Real-time Transport Protocol

¹⁰ IPsec – Internet Protocol Security

¹¹ TLS – Transport Layer Security

¹² NAT – Network Address Translation

¹³ IKEv1 – Internet Key Exchange version 1

¹⁴ RTCP – RTP Control Protocol

¹⁵ SSH – Secure Shell

¹⁶ SFTP – SSH File Transfer Protocol

¹⁷ SNMP – Simple Network Management Protocol

¹⁸ HTTPS – Hypertext Transfer Protocol Secure

¹⁹ UDP – User Datagram Protocol

²⁰ TCP – Transmission Control Protocol

²¹ DNS – Domain Name System

²² ENUM – E.164 Number Mapping

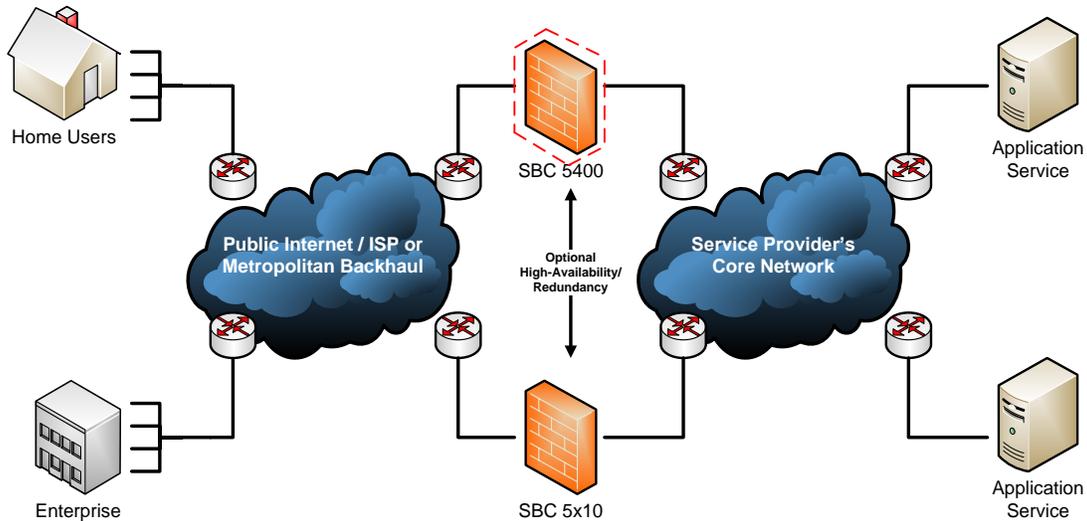


Figure 2 – A Typical Deployment Scenario of SBC 5400

Management of the SBC 5400 Session Border Controller is accomplished via:

- Command Line Interface (CLI), which is accessible remotely via SSH over Ethernet Management ports
- Web-based Graphical User Interface (GUI) called Embedded Management Application (EMA), which is accessible remotely via HTTPS over Ethernet management ports
- SNMPv3 traps and polling, which are used only for non-security relevant information about the module’s state and statistics

These management interfaces provide authorized operators access to the module for configuration and management of all facets of the module’s operation, including system configuration, troubleshooting, security, and service provisioning. Using any of the management interfaces, an operator is able to monitor, configure, control, receive report events, and retrieve logs from the SBC 5400.

The SBC 5400 Session Border Controller is validated at the FIPS 140-2 section levels shown in Table 1 below.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A ²³
7	Cryptographic Key Management	1

²³ N/A – Not applicable

Section	Section Title	Level
8	EMI/EMC ²⁴	1
9	Self-tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The SBC 5400 Session Border Controller is a hardware cryptographic module with a multiple-chip standalone embodiment. The cryptographic module runs Sonus’ proprietary ConnexIP operating system (OS), and consists of firmware and hardware components enclosed in a secure, production-grade metal case. The main hardware components consist of integrated circuits, processors, memories, SSD²⁵, flash, DSP cards, power supplies, fans, and the enclosure containing all of these components. The overall security level of the module is 1. The cryptographic boundary of the SBC 5400 is defined by the SBC 5400 device enclosure, which encompasses all the hardware and firmware components.

The BMC is excluded from the security requirements of this standard, along with all supporting chips, circuitry and external ports connected to the BMC. Although it physically resides within the cryptographic boundary, the BMC is a completely independent computing platform, with its own CPU, RAM, flash, ports, and operating system.

Also excluded from the FIPS 140-2 requirements are the Small Form-Factor Pluggable (SFP) transceiver modules that can be connected to the SBC 5400’s media and HA ports. These are simply adapters to interface the SBC 5400’s ports to either copper-based or fiber-based wiring, depending on the customer need. The SFPs do not provide any cryptographic services, nor do they store or process any critical security parameters. The malfunction of the SFPs cannot cause a breach to the security of the module or the information protected by them.

The SBC 5400 implements cryptographic algorithms in the following providers:

- Sonus Cryptographic Library v3.1 (based on OpenSSL FIPS Object Module 2.0.16 with OpenSSL 1.0.2I)
- Sonus Cryptographic Media Processor v3.1 (based on the Cavium OCTEON II CN6880 network processor)

The SBC 5400 Session Border Controller uses the FIPS-Approved algorithm implementations in hardware (Network Processor) and firmware (Crypto Library) as listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
NP	Library					
#5676	-	AES ²⁶	FIPS PUB 197	CBC, CTR ²⁷	128, 192, 256	Encryption/decryption
			NIST SP 800-38D	GCM ²⁸	128, 256	Encryption/decryption

²⁴ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

²⁵ SSD – Solid State Drive

²⁶ AES – Advance Encryption Standard

²⁷ CTR – Counter

²⁸ GCM – Galois Counter Mode

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
NP	Library					
-	#5677	AES	FIPS PUB 197	CBC, CFB1 ²⁹ , CFB8, CFB128	128, 192, 256	Encryption/decryption
			NIST SP 800-38D	GCM	128, 256	Encryption/decryption
-	Vendor Affirmed	CKG ³⁰	NIST SP 800-133	-	-	Symmetric key generation
-	#2064	CVL ³¹	NIST SP 800-56A	ECC CDH ³² Primitive	All NIST-recommended curves	Shared secret computation
-	#2070	CVL	NIST 800-135rev1	SNMP		Key derivation <i>*No parts of the SNMP protocol, other than the KDF, have been tested by the CAVP.</i>
-	#2071	CVL	NIST SP 800-135rev1	SSH	-	Key derivation <i>*No parts of the SSH protocol, other than the KDF, have been tested by the CAVP.</i>
-	#2072	CVL	NIST SP 800-135rev1	TLSv1.2	-	Key derivation <i>*No parts of the TLS protocol, other than the KDF, have been tested by the CAVP.</i>
#2063	-	CVL	NIST SP 800-135rev1	SRTP ³³	-	Key derivation <i>*No parts of the SRTP protocol, other than the KDF, have been tested by the CAVP.</i>
-	#2295	DRBG ³⁴	NIST SP 800-90Arev1	CTR-based	128	Deterministic random bit generation
-	#1538	ECDSA ³⁵	FIPS PUB 186-4	PKG, PKV	All NIST-recommended curves	Key pair generation and verification
				SigGen, SigVer	All NIST-recommended curves	Digital signature generation and verification
#3779	-	HMAC ³⁶	FIPS PUB 198-1	SHA-1 ³⁷	-	Message authentication
-	#3780	HMAC	FIPS PUB 198-1	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	Message authentication

²⁹ CFB – Cipher Feedback

³⁰ CKG – Cryptographic Key Generation

³¹ CVL – Component Validation List

³² ECC CDH – Elliptic Curve Cryptographic Cofactor Diffie Hellman

³³ SRTP – Secure Real-Time Transport Protocol

³⁴ DRBG – Deterministic Random Bit Generator

³⁵ ECDSA – Elliptic Curve Digital Signature Algorithm

³⁶ HMAC – (keyed-) Hashed Message Authentication Code

³⁷ SHA – Secure Hash Algorithm

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
NP	Library					
-	Vendor Affirmed	PBKDF2 ³⁸	NIST SP 800-132	Option 1	-	Key derivation
-	#3055	RSA ³⁹	FIPS PUB 186-4	SigGenPKCS1.5 ⁴⁰	2048	Digital signature generation
				SigVerPKCS1.5	1024, 2048	Digital signature verification
				KeyGen9.31	2048	Key pair generation
#4549		SHS ⁴¹	FIPS PUB 180-4	SHA-1	-	Message digest
-	#4550	SHS	FIPS PUB 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	Message digest
#2845	-	Triple-DES ⁴²	NIST SP 800-67	TCBC	Keying option 1	Encryption/decryption
-	#2846	Triple-DES	NIST SP 800-67	TCBC	Keying option 1	Encryption/decryption

The vendor affirms the following cryptographic security methods:

- As per *NIST SP 800-133*, the module uses its FIPS-Approved counter-based DRBG to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module’s DRBG is seeded via `/dev/random`, a non-deterministic random number generator (NDRNG) internal to the module.
- As per *NIST SP 800-132*, the module uses PBKDF2 option 1 to derive the Certificate Load Key. This function takes an input salt that is 128 bits in length with a passphrase containing at least eight characters (following the password complexity requirements in section 3.4 below) and produces a random value of 128 bits (when producing keys for AES) or 168 bits (when producing keys for Triple DES). In addition, the function has an iteration count of 2048. The underlying pseudorandom function used in this derivation is SHA-1.

The module implements the non-Approved but allowed algorithms shown in Table 3.

Table 3 – Allowed Algorithms

Algorithm	Standard	Caveat	Use
Diffie-Hellman (CVL Certs. #2071 and #2072)	NIST SP 800-56A	key establishment methodology provides 112 bits of encryption strength	Key agreement
Elliptic Curve Diffie-Hellman (ECDH) (CVL Certs. #2064, #2071, and #2072)	NIST SP 800-56A	key establishment methodology provides between 112 and 256 bits of encryption strength	Key agreement

³⁸ PBKDF2 – Password-Based Key Derivation Function 2

³⁹ RSA – Rivest Shamir Adleman

⁴⁰ PKCS – Public Key Cryptography Standard

⁴¹ SHS – Secure Hash Standard

⁴² DES – Data Encryption Standard

Algorithm	Standard	Caveat	Use
MD5 ⁴³	-	-	TLS protocol handshake
NDRNG ⁴⁴	-	-	Seeding for the FIPS-Approved DRBG
RSA	NIST SP 800-56B	key establishment methodology provides 112 bits of encryption strength	Key transport

The module implements 1024-bit RSA key pair generation and digital signature generation, which provides less than 112 bits of encryption strength, and thus is considered non-compliant. Use of this algorithm with this key size is prohibited when operating in FIPS mode. See section 3.4 for details. The module also implements a non-compliant IKE KDF, which is used for establishing IPsec sessions. This algorithm is only to be used while the module is operating in its non-Approved mode (see section 3.5 below for details).

Additional information concerning DSA, ECDSA, Diffie-Hellman key establishment, RSA, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in *NIST SP 800-131Arev1*.

2.3 Module Ports and Interfaces

The module's design separates the physical ports and interfaces into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Data input/output are the packets utilizing the services provided by the module. These packets enter and exit the module through the Ethernet media, management, and HA⁴⁵ interfaces. Control input consists of configuration or administration data entered into the module through the Command Line Interface (CLI) and Web GUI over Ethernet management interfaces, USB, and HA ports. Status output consists of the status relayed over the Ethernet management interfaces, HA ports, and also displayed via LEDs⁴⁶ and through the log information accessible over Ethernet management ports.

2.3.1 Front Bezel Interfaces

The physical LEDs and ports/interfaces found on the front bezel of the SBC 5400 Session Border Controller are shown in Figure 3 below.

⁴³ MD5 – Message Digest 5

⁴⁴ NDRNG – Non Deterministic Random Number Generator

⁴⁵ HA – High Availability

⁴⁶ LED – Light Emitting Diode

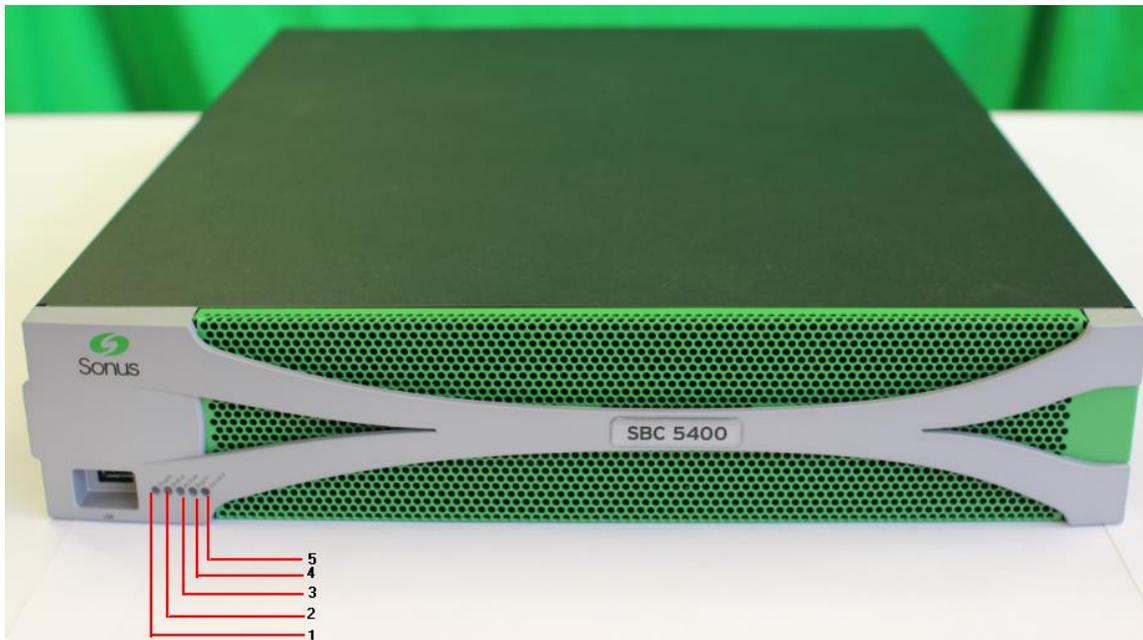


Figure 3 – LEDs and Ports/Interfaces (Front Bezel)

Table 4 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2.

Table 4 – FIPS 140-2 Logical Interface Mappings (Front Bezel)

No.	Physical Port/Interface	Description	FIPS 140-2 Logical Interface
1	Power LED	Power status indicator: <ul style="list-style-type: none"> GREEN: all power on OFF: BMC power on or chassis power off 	<ul style="list-style-type: none"> Status out
2	Status LED	Module status indicator: <ul style="list-style-type: none"> GREEN: application is running AMBER: application startup has not completed, or the application has been shutdown OFF: application is not running 	<ul style="list-style-type: none"> Status out
3	Active LED	Module Redundancy State indicator: <ul style="list-style-type: none"> GREEN: active and protected AMBER: active but unprotected OFF: not active 	<ul style="list-style-type: none"> Status out
4	Alarm LED	Module critical/major failure indicator: <ul style="list-style-type: none"> RED: critical alarm AMBER: major alarm OFF: no alarm conditions 	<ul style="list-style-type: none"> Status out

No.	Physical Port/Interface	Description	FIPS 140-2 Logical Interface
5	Locator LED	Module identifier indicator: <ul style="list-style-type: none"> GREEN: fan module is working OFF: fan module is not working 	<ul style="list-style-type: none"> Status out
-	USB Port	USB v2.0 interface	<ul style="list-style-type: none"> Control in

2.3.2 Front Panel Interfaces

The physical LEDs and ports/interfaces found behind the front bezel of the SBC 5400 Session Border Controller are shown in Figure 4 below.

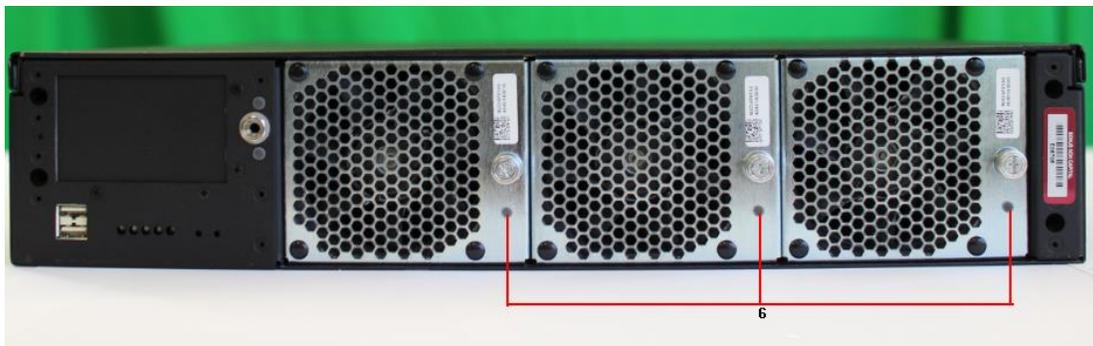


Figure 4 – LEDs and Ports/Interfaces (Front Panel)

Table 5 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2.

Table 5 – FIPS 140-2 Logical Interface Mappings (Front Panel)

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Fan Control LED	1 per fan	Fan module indicator: <ul style="list-style-type: none"> GREEN: fan module is working OFF: fan module is not working 	<ul style="list-style-type: none"> Status out

Please note that the front bezel LEDs also show on the module’s front panel when the bezel is not mounted.

2.3.3 Rear Panel Interfaces

The physical ports and interfaces found on the rear panel of the SBC 5400 Session Border Controller are shown in Figure 5 below.

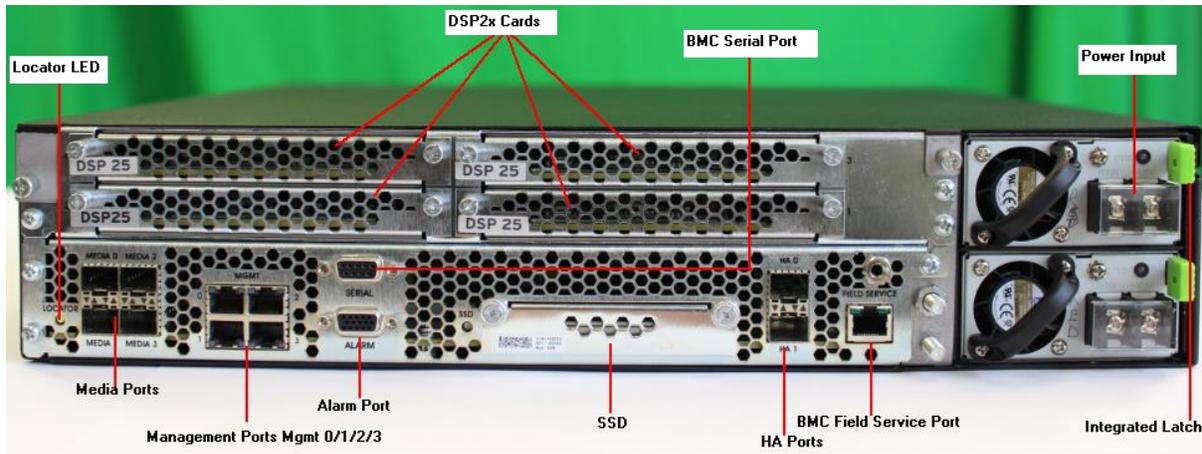


Figure 5 – LEDs and Ports/Interfaces (Rear Panel)

Table 6 provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2.

Table 6 – FIPS 140-2 Logical Interface Mappings (Rear Panel)

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Management Ports	4 x 100 Mbps ⁴⁷	Copper RJ-45 Ethernet ports which process management traffic and perform protocol termination	<ul style="list-style-type: none"> Data in Data out Control in Status out
Management Port LEDs	2 per port	Indicator of management port link and activity status: <ul style="list-style-type: none"> The Link LED is solid green when the link is up. The Activity LED is Flashing Green when there is activity present on the port. 	<ul style="list-style-type: none"> Status out
Locator LED	1	Module identifier indicator	<ul style="list-style-type: none"> Status out
Media Ports	4 x 1 Gbps ⁴⁸ (one port is 10 Gbps-capable)	Copper SFP or fiber SFP Ethernet ports for media and signaling traffic	<ul style="list-style-type: none"> Data in Data out
Media Port LEDs	2 per port	Indicator of media port link and activity status: <ul style="list-style-type: none"> The Link LED is solid green when the link is up. The Activity LED is Flashing Green when there is activity present on the port. 	<ul style="list-style-type: none"> Status out

⁴⁷ Mbps – Megabits per second

⁴⁸ Gbps – Gigabits per second

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
High Availability Ports	2 x 1 Gbps	Copper SFP or fiber Ethernet SFP ports for redundancy synchronization traffic.	<ul style="list-style-type: none"> • Data in • Data out • Control in • Status out
High Availability Port LEDs	2 x 1 Gbps	Indicator of HA port link and activity status: <ul style="list-style-type: none"> • The Link LED is solid green when the link is up. • The Activity LED is Flashing Green when there is activity present on the port. 	<ul style="list-style-type: none"> • Status out
Serial Port	1	An RS-232 port used by BMC	N/A
Field Service Ethernet Port	1 x 100 Mbps	An Ethernet port for servicing in the field	N/A
Field Service Ethernet Port LEDs	2 per port	Indicator of field service port link and activity status: <ul style="list-style-type: none"> • The Link LED is solid green when the link is up. • The Activity LED is Flashing Green when there is activity present on the port. 	<ul style="list-style-type: none"> • Status out
Power LED	1 per power supply	Indicator of power supply status: <ul style="list-style-type: none"> • OFF: No power input to the supply • AMBER: Power supply fault • BLINKING AMBER: Main system power output fault • BLINKING GREEN: Standby power to BMC is ON but main system power is not enabled • GREEN: Both standby power to BMC and main system power are on and OK. 	<ul style="list-style-type: none"> • Status out

NOTE: Each module also includes a back panel alarm port. This port is not operational, and thus provides no facility for input or output.

2.4 Roles, Services, and Authentication

The sections below describe the module’s roles and services, and define any authentication methods employed.

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two roles that operators may assume:

- **Crypto Officer** – The CO is responsible for initializing the module for first use, which includes the configuration of passwords, public and private keys, and other CSPs. The CO is also responsible for the management of all keys and CSPs, including their zeroization. Lastly, the CO is the only operator that can configure the module into FIPS-Approved mode of operation. The CO also has access to all User services.

- User – The User has read-only privileges and can show the status and statistics of the module, show the current status of the module, and connect to the module remotely using HTTPS and SSH.

2.4.2 Operator Services

Descriptions of the services available to the Crypto Officer role and User role are provided in the Table 7 below. The keys and CSPs listed in Table 7 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 7 – Authorized Operator Services

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Commission the module	✓		Commission the module by following the Security Policy guidelines	None	None	None
Manage SBC license	✓		Installs the license to enable SBC features; delete or update license; view current license status	Command	Status output	None
Configure the SBC system	✓		Define network interfaces and settings; set protocols; configure authentication information; define policies and profiles	Command and parameter	Command response/ Status output	None
Configure routing policy and control services	✓		Configure IP network parameters and profiles for signaling, media, call routing, call services, zone, IP ACL ⁴⁹ rules, NTP ⁵⁰ and DNS ⁵¹ servers	Command and parameters	Command response/ Status output	None
Configure Crypto Suite Profile	✓		Select crypto suites for SRTP, SRTCP, and SIP communication	Command and parameters	Command response/ Status output	None

⁴⁹ ACL – Access Control List

⁵⁰ NTP – Network Time Protocol

⁵¹ DNS – Domain Name System

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Configure Call Data Record (CDR)	✓		Configure log file behavior	Command and parameters	Command response/ Status output	None
Manage users	✓		Create, edit and delete users; define user accounts and assign permissions.	Command and parameters	Command response/ Status output	Crypto Officer Password – R/W/X User Password – R/W/X
Manage user sessions	✓		Terminate User sessions	Command and parameters	Command response/ Status output	TLS Session Key – W
Change password	✓	✓	Modify existing login passwords	Command and parameters	Command response/ Status output	Crypto Officer Password – R/W User Password – R/W
Load certificate	✓		Load new certificates	Command	Command response/ Status output	Certificate Load Key – W/X CA ⁵² Public Key – R/W TLS Private Key – R/W TLS Public Key – R/W TLS Peer Public Key – R/W SSH Peer Public Key – R/W
Run script	✓		Run a script file (a text file containing a list of CLI commands to execute in sequence)	Command	Command response/ Status output	None (service may potentially access CSPs indirectly via scripted CLI commands)
Perform self tests	✓		Perform on-demand Self-Tests	Command	Command response/ Status output	All ephemeral keys and CSPs – W
Perform network diagnostics	✓	✓	Monitor connections (e.g. ping)	Command	Command response/ Status output	None
Show status	✓	✓	Show the system status, Ethernet status, FIPS Approved mode, alarms, system identification and configuration settings of the module	Command	Command response/ Status output	None
View Event Log	✓		View event status messages	Command	Command response/ Status output	None
Zeroize keys	✓		Zeroize all keys and CSPs	Command	Command response/ Status output	All ephemeral and persistent keys and CSPs – W

⁵² CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Upgrade firmware	✓		Load new firmware and performs an integrity test using an RSA digital signature	Command	Command response/ Status output	Firmware Load Authentication Key – R/X
Perform keying of CDB ⁵³ Key	✓		Generate CDB key	Command and parameters	Command response/ Status output	CDB key – W/X
Reboot/Reset	✓		Reboot or reset the module	Command	Command response/ Status output	CSPs stored in SDRAM – W
Establish TLS session	✓	✓	Establish web session using TLS protocol	Command	Command response/ Status output	AES-GCM IV – R/W/X Diffie-Hellman Public Key – R/X Diffie-Hellman Private Key – X ECDH Public Component – R/X ECDH Private Component – X TLS Private Key – W/X TLS Public Key – W/X TLS Peer Public Key – R/X TLS Pre-Master Secret – W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – W/X
Establish SSH session	✓	✓	Establish remote session using SSH protocol	Command	Command response/ Status output	AES-GCM IV – R/W/X Diffie-Hellman Public Key – R/X Diffie-Hellman Private Key – X ECDH Public Component – R/X ECDH Private Component – X SSH Private Key – W/X SSH Public Key – W/X SSH Peer Public Key – R/X SSH Shared Secret – W/X SSH Session Key – R/W/X SSH Authentication Key – W/X
Establish SRTP session	✓	✓	Establish a SIP/TLS session using SRTP protocol	Command	Command response/ Status output	AES-GCM IV – R/W/X SRTP Master Key – R/X SRTP Symmetric Key – W/X SRTP Authentication Key – W/X
SNMPv3 traps		✓	Provides system condition information	None	Status output	SNMPv3 Session Key – R/W/X SNMPv3 HMAC Key – R/W/X

⁵³ CDB – Configuration Database

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Encryption/ decryption service	✓	✓	Encrypt or decrypt user data, keys, or management traffic	Command and parameters	Command response	TLS Session Key – X SSH Session key – X

All services listed above require the operator to assume a role, and the module authenticates the role before providing any of these services.

2.4.3 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 8 lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

Table 8 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize keys and CSPs	Power cycling using power connectors	Status output	All ephemeral keys and CSPs – W
Perform on-demand self-tests	Perform power-up self-tests on demand	Cycle power using power connectors	Status output	All ephemeral keys and CSPs – W
Authenticate	Used for operator logins to the module	Command	Status output	Crypto Officer Password – X User Password – X RADIUS Shared Secret – W/X TLS Public Key – X

2.4.4 Authentication

The module supports role-based authentication and multiple concurrent operators. Operator authentication is managed either from a local database or a configured remote RADIUS⁵⁴ server. Upon initial module configuration, local authentication is enabled by default. If both methods are enabled, remote authentication takes priority and is attempted first. If the remote authentication fails, the module attempts local authentication. The login attempt is rejected if both attempts fail.

All module operators authenticate using a username and password. The module also supports RSA digital certificate authentication of operators during Web GUI/HTTPS (TLS) access. Table 9 lists the authentication mechanisms used by the module. The strength calculation below provides minimum strength based on password policy described in Section 3.4.

⁵⁴ RADIUS – Remote Authentication Dial In User Service

Table 9 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Password	<p>The minimum length of the password is eight characters, with 95 different case-sensitive alphanumeric characters and symbols possible for usage. The chance of a random attempt falsely succeeding is:</p> <p>=1 per 95^8 possible passwords =1 per 6,634,204,312,890,625 which is a lesser probability than 1 per 1,000,000 as required by FIPS 140-2.</p> <p>The fastest network connection over Ethernet Interface supported by the module is 100 Mbps. Hence, at most $(10 \times 10^7 \times 60) = (6 \times 10^9) = 6,000,000,000$ bits of data can be transmitted in one minute. The probability that a random attempt will succeed or a false acceptance will occur in one minute is:</p> <p>=1 per $(95^8 \text{ possible passwords}) / ((6 \times 10^9 \text{ bits per minute}) / 64 \text{ bits per password})$ =1 per $(95^8 \text{ possible passwords} / 93,750,000 \text{ passwords per minute})$ =1 per 70,764,846 which is a lesser probability than 1 per 100,000 as required by FIPS 140-2.</p>
Public Key Certificates	<p>The module supports RSA digital certificate authentication of users during Web GUI/HTTPS (TLS) access. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is:</p> <p>=1 per 2^{112} =1 per 5.19×10^{33} which is a lesser probability than 1 per 1,000,000 as required by FIPS 140-2.</p> <p>The fastest network connection over the Media ports supported by the module is 10 Gbps. Hence, at most $(10 \times 10^9 \times 60) = (6 \times 10^{11}) = 600,000,000,000$ bits of data can be transmitted in one minute. The probability that a random attempt will succeed or a false acceptance will occur in one minute is:</p> <p>=1 per $(2^{112} \text{ possible keys} / ((6 \times 10^{11} \text{ bits per minute}) / 112 \text{ bits per key}))$ =1 per $(2^{112} \text{ possible keys} / 5,357,142,857 \text{ keys per minute})$ =1 per 96.92×10^{22} which is a lesser probability than 1 per 100,000 as required by FIPS 140-2.</p>

The feedback of authentication data to a user is obscured during an operator’s entry of authentication credentials. The module provides feedback by displaying a “rounded dot” (●) symbol when an operator is entering his password over EMA login, while no feedback is provided for CLI login.

The module provides the ability for an operator to change roles. In order to change roles, an operator is required to first log out and then re-authenticate with an account with appropriate permissions for the desired role.

The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. The authenticated CO can modify their own authentication credentials as well as the credentials of the Users, while the Users have the ability to modify their own authentication data only.

2.5 Physical Security

All CSPs are stored and protected within the SBC 5400 Session Border Controller's production-grade enclosure. The main chassis enclosure consists of a removable upper cover, two (2) removable power supplies, and up to four (4) DSPs. The removable upper cover is secured to the main enclosure with screws.

All of the components within the module are production grade with standard passivation.

2.6 Operational Environment

The module employs an Intel Xeon (Ivy Bridge) processor running Sonus' proprietary ConnexIP OS. The network processor is a Cavium OCTEON II CN6880. This operational environment does not provide a general-purpose OS to the operator. The operational environment is not modifiable by the operator, and only the module's signed image can be executed. All firmware upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade. If the signature test fails, the new firmware is ignored and the current firmware remains loaded.

NOTE: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.7 Cryptographic Key Management

To support TLS, the module employs the following certificate management techniques:

- Local – RSA public/private key pairs and Certificate Signing Requests (CSRs) for the SBC 5400 are generated on an external workstation. Each CSR is signed with workstation's public key and then submitted to a Certificate Authority (CA). The workstation receives the issued certificate back from the CA, then stores the key pair and certificate in a PKCS #12-formatted file. This certificate file is then encrypted (using 128-bit AES or Triple-DES in CBC mode) and sent to the SBC 5400 via SSH for installation.
- Local-Internal – The SBC 5400 generates its RSA key pairs and Certificate Signing Requests (CSR) internally. The certificate request is signed with SBC 5400's public key and then sent to a CA. The issued certificate is received back from the CA and then installed on the SBC 5400.
- Remote – Remote certificates are credentials belonging to CAs. The CA certificates contain public keys only; they do not contain the associated private keys. The CA certificates are Distinguished Encoding Rules (DER) format files.

The module supports the CSPs described in Table 10 below.

Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Config Database (CDB) Key	Triple-DES 168-bit key	Generated internally via FIPS-Approved DRBG	Never exits the module	Plaintext in SSD	When re-keyed over CLI or EMA; When appliance is re-imaged; Upon command via CLI or EMA	Encryption of RSA and ECDSA private keys and preshared secrets for RADIUS in CDB
CA Public Key	2048-bit RSA key	Generated externally, imported in DER ⁵⁵ file format	Never exits the module	Plaintext in RAM		Verification of Certificate Authority signatures
ECDH Private Component	Private component of ECDH protocol	Generated internally	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Establishment of SSH and TLS session keys
ECDH Public Component	Public component of ECDH protocol	[for the module] Generated internally [for a peer] Generated externally, entered into the module (in certificate form) in plaintext	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Establishment of SSH and TLS session keys
Diffie-Hellman Private Key	2048-bit DH key	Generated internally	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Generation of SSH and TLS shared secrets

⁵⁵ DER – Distinguished Encoding Rules

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Diffie-Hellman Public Key	2048-bit DH key	[for the module] Generated internally [for a peer] Generated externally, entered into the module (in certificate form) in plaintext	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Generation of SSH and TLS shared secrets
SSH Private Key	2048-bit RSA key	Generated internally via FIPS-Approved DRBG	Never exits the module	Encrypted in the CDB on SSD	Command via CLI or EMA	Authentication during SSH session negotiation
SSH Public Key	1024/2048-bit RSA key	Generated internally via FIPS-Approved DRBG	Exits the module in plaintext form	Plaintext in the CDB on SSD	Command via CLI or EMA	Authentication during SSH session negotiation 1024-bit key is used for signature verification only
SSH Peer Public Key	1024/2048-bit key	Imported in plaintext	Never exits the module	Plaintext in the CDB on SSD	Command via CLI or EMA	Authentication during session negotiation
SSH Shared Secret	Shared secret	Derived internally via DH/ECDH shared secret computation	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Derivation of the SSH Session Key and SSH Authentication Key
SSH Session Key	128/192/256 AES-CBC, 128/192/256 AES-CTR, 128/256-bit AES-GCM, or 168-bit Triple-DES CBC key	Derived internally via SSH KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Encryption and decryption of SSH session packets
SSH Authentication Key	160-bit (minimum) HMAC key	Derived internally via SSH KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Authentication of SSH session packets

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Private Key	<p>[for authentication using RSA certificates] 2048-bit RSA private key</p> <p>[for authentication using ECDSA certificates] All NIST-recommended ECDSA curves</p>	<p>[for local-internal certificates] Generated internally via FIPS-Approved DRBG</p> <p>[for local certificates] Generated externally, imported via PKCS #12 file format in encrypted form</p>	Never exits the module	Encrypted in the CDB on SSD	Command via CLI or EMA	Authentication during TLS key negotiation
TLS Public Key	<p>[for authentication using RSA certificates] 2048-bit RSA public key</p> <p>[for authentication using ECDSA certificates] All NIST-recommended ECDSA curves</p>	<p>[for local-internal certificates] Generated internally via FIPS-Approved DRBG</p> <p>[for local certificates] Generated externally, imported via PKCS #12 file format in encrypted form</p>	Exits the module via digital certificate in plaintext form	Plaintext in the CDB on SSD	Command via CLI or EMA	Authentication during TLS key negotiation
TLS Peer Public Key	<p>[for authentication using RSA certificates] 2048-bit RSA public key</p> <p>[for authentication using ECDSA certificates] All NIST-recommended curves</p>	Generated externally, imported in certificate form in plaintext	Never exits the module	Plaintext in the CDB on SSD	Command via CLI or EMA	Certificate-based authentication during TLS key negotiation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Pre-Master Secret	[for RSA cipher suites] 384-bit random value [for DH/ECDH cipher suites] DH/ECDH shared secret	[for RSA cipher suites and module acting as client] Generated internally via FIPS-Approved DRBG [for RSA cipher suites and module acting as server] Generated externally, imported in encrypted form via RSA key transport [for DH/ECDH cipher suites] Derived internally via DH/ECDH shared secret computation	[for RSA cipher suites and module acting as client] Exits the module in encrypted form via RSA key transport [for RSA cipher suites and module acting as server] Never exits the module [for DH/ECDH cipher suites] Never exits the module	Plaintext in RAM	Upon module reboot; Upon completion of TLS Master Secret computation	Derivation of the TLS Master Secret
TLS Master Secret	384-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128/256-bit AES key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Encryption and decryption of TLS session packets
TLS Authentication Key	160-bit (minimum) HMAC key	Derived internally using the TLS Master Secret via the TLS KDF	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Authentication of TLS session packets
SRTP Master Key	128/192/256-bit shared secret	Generated externally, imported in encrypted form via a secure SIP/TLS session	Exits in encrypted form	Plaintext in RAM	Upon module reboot; Upon session termination	Peer Authentication, Session and Authentication keys derivation for SRTP session

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SRTP Session Key	128/192/256-bit AES-CTR or 128/256-bit AES GCM key	Generated internally using SRTP Master Key	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Encryption or decryption during SRTP session
SRTP Authentication Key	160-bit HMAC key	Generated internally using SRTP Master Key	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Authentication of SRTP session packets
RADIUS Shared Secret	Shared secret (alpha-numeric string)	Entered electronically by Crypto Officer	Never exits the module	Encrypted in the CDB on SSD	Upon command via CLI or EMA	Peer authentication of RADIUS messages
DRBG Seed	256-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Seed value generated by the DRBG
DRBG Entropy Input String ⁵⁶	512-bit value	Generated internally from various module resources by the NDRNG	Never exits the module	Plaintext in RAM	Upon module reboot; Upon session termination	Entropy material for DRBG seed generation
DRBG Key Value	Internal DRBG state value	Generated internally	Never exits the module	Plaintext in RAM	Upon module reboot	Generation of random number
DRBG 'V' Value	Internal DRBG state value	Generated internally	Never exits the module	Plaintext in RAM	Upon module reboot	Generation of random number
SFTP Private Key	2048-bit RSA key	Generated internally via FIPS-Approved DRBG	Never exit the module	Stored in the CDB on SSD – encrypted for the certificates; stored outside CDB on SSD – plaintext for SSH	Upon command via CLI or EMA	Used for SFTP key negotiation

⁵⁶ With a *min-entropy* value of 0.72016, the minimum number of bits of entropy generated by the module for use in key generation is 368.7 bits per each 512-bit request.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SFTP Public Key	1024/2048-bit RSA key	[for the module] Generated internally [for a peer] Generated externally, entered into the module in plaintext form	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in the CDB on SSD	Upon command via CLI or EMA	Used for SFTP key negotiation 1024-bit key is used for signature verification only
SNMPv3 Session Key	128-bit AES-CFB or 168-bit Triple-DES key	Generated externally, imported in encrypted form via a secure TLS or SSH session	Exits in encrypted form (over TLS session) within configuration data when performing configuration backup	Plaintext in the CDB on SSD	Upon command via CLI or EMA	Encrypting SNMPv3 packets
SNMPv3 Authentication Key	160-bit HMAC key	Generated externally, imported in encrypted form via a secure TLS or SSH session	Exits in encrypted form (over TLS session) within configuration data when performing configuration backup	Plaintext in the CDB on SSD	Upon command via CLI or EMA	Authenticating SNMPv3 packets
Crypto Officer password	Alphanumeric string (minimum of eight characters)	Initial password generated internally using FIPS-Approved DRBG; password changes entered into module via a console port or over SSH	Initially generated password provided to the CO on CLI/EMA over encrypted session; changed password never exits the module	Plaintext ⁵⁷ on SSD and in RAM	When the password is updated with a new one	Authenticating the Crypto Officer to the module
User password	Alphanumeric string (minimum of eight characters)	Initial password generated internally using DRBG; password changes entered into module via a console port or over SSH	Initially generated password provided to the User on CLI/EMA over encrypted session; changed password never exits the module	Plaintext on SSD and in RAM	When the password is updated with a new one	Authenticating the User to the module

⁵⁷ CO and User passwords are obfuscated by the operating system and stored on the SSD. They are temporarily loaded into the memory in obfuscated form for comparison during a login.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Software Load Authentication Key	2048-bit key RSA public key	Embedded in release image	Never exits the module	Stored in flash memory	The flash location is write-protected in hardware at the factory (i.e., not writeable by end user) and is not zeroized.	Verifying the RSA signature of the digest of a new software load package
Certificate Load Key*	128/256-bit AES or 168-bit Triple-DES key	Derived internally via PBKDF2 (option 1)	Never exits the module	Plaintext in RAM	Upon module reboot	Decrypting PKCS #12 certificate files when imported from an external workstation
AES GCM IV ⁵⁸	96-bit IV	Generated internally via FIPS-Approved DRBG	Never exits the module	Plaintext in volatile RAM	Upon module reboot	IV input to AES-GCM function

*Keys derived from the PBKDF2 function shall only be used for storage applications.

⁵⁸ IV – Initialization Vector

The AES-GCM IV⁵⁹ is used in the following protocols:

- TLS – For TLS, the AES-GCM IV is internally generated deterministically in compliance with TLSv1.2 GCM cipher suites as specified in RFC 5288 and Section 8.2.1 of NIST SP 800-38D. Per RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key.
- SSH – For SSH, the AES-GCM IV is internally generated at its entirety randomly using an Approved DRBG, whose seed is generated inside the module’s physical boundary. Per NIST SP 800-38D, the IV length is 96 bits.
- SRTP – For SRTP, the AES-GCM IV is internally generated at its entirety randomly using an Approved DRBG, whose seed is generated inside the module’s physical boundary. Per NIST SP 800-38D, the IV length is 96 bits.

2.8 EMI / EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self-Tests

The module performs power-up self-tests, conditional self-tests, and critical function tests. These tests are described in the sections that follow.

2.9.1 Power-Up Self-Tests

The SBC 5400 Session Border Controller performs the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithm implementations:

- Firmware integrity tests using SHA-256 (for OS, SonusDB, EMA, Crypto Library, and SBC firmware components)
- Network Processor driver algorithm tests:
 - AES encrypt KAT⁶⁰
 - AES decrypt KAT
 - HMAC SHA-1 KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
- Crypto Library algorithm tests:
 - AES encrypt KAT
 - AES decrypt KAT
 - AES GCM encrypt KAT
 - AES GCM decrypt KAT
 - Triple-DES encrypt KAT

⁵⁹ IV – Initialization Vector

⁶⁰ KAT – Known Answer Test

- Triple-DES decrypt KAT
- HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512 KAT
- CTR_DRBG KAT
- RSA signature generation KAT
- RSA signature verification KAT
- ECDSA Pair-wise Consistency Test
- ECC CDH Primitive “Z” Computation KAT

NOTE: The firmware integrity tests using SHA-256 utilize (and thus test) the full functionality of the SHA-256 algorithm; thus, no independent KAT for the SHA-256 implementation is required.

The CO or User can run the module’s power-up self-tests at any time by power-cycling the module or issuing a reboot command over the module’s Management interfaces. Also, the module can be made to perform power-up self-tests by disconnecting and reconnecting power connectors to the module; and for this service, an operator is not required to assume an authorized role.

2.9.2 Conditional Self-Tests

The SBC 5400 Session Border Controller performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for the DRBG (Crypto Library)
- CRNGT for the NDRNG entropy source (Crypto Library)
- Firmware Load Test using RSA signature verification (for OS, SonusDB, EMA, and SBC)
- RSA Pair-wise Consistency Test (Crypto Library)
- ECDSA Pair-wise Consistency Test (Crypto Library)
- ECC CDH public key assurance test (Crypto Library)

2.9.3 Critical Functions Self-Tests

The SBC 5400 Session Border Controller implements the counter-based DRBG (specified in *NIST SP 800-90Arev1*) as its random number generator. The DRBG specification requires that certain critical functions be tested conditionally to ensure the security of the DRBG. Therefore, the following critical function tests are implemented by the cryptographic module:

- Instantiate Critical Function Test
- Generate Critical Function Test
- Reseed Critical Function Test
- Uninstantiate Critical Function Test

2.9.4 Self-Test Failure Handling

Upon failure of the conditional firmware load test, the module enters a “Soft Error” state and disables all access to cryptographic functions and CSPs. This is a transitory error state, during which the error status is recorded to the system log file and/or event audit log file. Upon failure of this self-test, the CO may choose to reject or continue with the firmware load. Rejecting the load will abort the load process, clear the error condition, and the module will continue normal operations with the currently-loaded firmware. Choosing to continue will load the firmware, clear the error condition, and the module will continue operating with the currently-loaded firmware until the next reboot.

Upon failure any other power-up self-test, conditional self-test, or critical function test, the module will go into a “Critical Error” state and disable all access to cryptographic functions and CSPs. All data outputs are inhibited, and a permanent error status will be recorded to the system log file and/or event audit log file. The task that invoked the failed self-test will be suspended, and the current operation will not complete. The management interfaces will not respond to any commands while the module is in this state. The CO must reboot the module to clear the error condition and return to a normal operational state.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The SBC 5400 Session Border Controller meets overall Level 1 requirements for FIPS 140-2. The sections below describe how to ensure that the module is running securely. Please note that physical access to the module shall be limited to authorized operators only.

3.1 Initial Setup

The module is delivered in an uninitialized factory state, and requires first-time configuration in order to operate in its FIPS-Approved mode. Physical access to the module shall be limited to the Crypto Officer, and the CO shall be responsible for putting the module into the Approved mode.

The Crypto Officer shall receive the module from Sonus via trusted couriers (e.g. United Parcel Service, Federal Express, and Roadway). On receipt, the Crypto Officer must check the package for any irregular tears or openings. If any such damage exists, the CO shall indicate that on the shipping document of the carrier and contact Sonus Networks, Inc. immediately for instructions. The CO shall also retain the packing list, making sure all the items on the list are present (including all the components of the universal rack mount kit that is shipped with the module).

The Crypto Officer is responsible for all initial setup activities, including configuring the platform and installing the SBC application software. For detailed guidance regarding the use of the module's management interfaces for accomplishing these activities, please see the [SBC Core 6.2.x Documentation](#) webpage on Sonus' online Documentation and Support Portal and refer to the following document entries:

- [EMA User Guide](#)
- [CLI Reference Reference](#)

The following sections provide references to step-by-step instructions for the installation of the SBC 5400 device and software, as well as the steps necessary to configure the module for its FIPS-Approved mode of operation.

3.1.1 Hardware Installation and Commissioning

To setup the SBC 5400, the CO must follow the instructions found under the online document entry "[Installing SBC 5400 Hardware](#)", which provides detailed guidance for installing rack mount kits, mounting the SBC chassis, attaching the front bezel, connecting cables and power, and powering on the SBC.

Once these steps have been completed, the SBC hardware is considered to be installed and commissioned.

3.1.2 Application Installation and Configuration

The next steps are to configure the management interfaces and to install the SBC application software. The CO must follow the instructions under the online document entry "[Installing SBC 5400 Software](#)", which provides detailed guidance for configuring the platform and installing the application software.

Once the network settings are correctly configured for the module, continue to Section 3.1.3 in this document to configure SBC module for the FIPS-Approved mode.

3.1.3 Enabling FIPS-Approved Mode

To set the module into its FIPS mode of operation, the CO may use the CLI or the EMA.

To enable FIPS mode using the CLI, the CO shall complete the following procedure:

1. Log in to the CLI using the default username “admin” and password “admin”.
2. Execute the following commands:

```
> configure private
% set profiles security tlsProfile defaultTlsProfile v1_0 disabled v1_1 disabled v1_2
enabled
% set profiles security EmaTlsProfile defaultEmaTlsProfile v1_0 disabled v1_1 disabled
v1_2 enabled
% set oam snmp version v3only
% set system admin <system name> fips-140-2 mode enabled
% commit
```

To enable FIPS mode using the EMA, the CO shall complete the following procedure (note that the EMA does not include all of the commands necessary to enable FIPS mode; the CLI must be used to complete the procedure):

1. Log in to the EMA using the default username “admin” and password “admin”.
2. Using the EMA menu bar, navigate to **All -> Profiles -> Security -> TLS Profile**. The **TLS Profile** window is displayed, with the **TLS Profile List** pane.
3. Select the radio button corresponding to the defaultTlsProfile. The **Edit Selected TLS Profile** pane is displayed.
4. Set the fields V1_0 and V1_1 to “Disabled”. Set the field V1_2 to “Enabled”.
5. Click **Save** to save the changes.
6. Using the EMA menu bar, navigate to **All -> Profiles -> Security -> EMA TLS Profile**. The **EMA TLS Profile** window is displayed, with the **EMA TLS Profile List** pane.
7. Select the radio button corresponding to the defaultEmaTlsProfile. The **Edit Selected EMA TLS Profile** pane is displayed.
8. Set the fields V1_0 and V1_1 to “Disabled”. Set the field V1_2 to “Enabled”.
9. Click **Save** to save the changes.
10. Using the EMA menu bar, navigate to **All -> OAM -> Snmp**. The **Snmp** window is displayed, with the **Edit Snmp** pane.
11. Set the Version field to “V3only”.
12. Click **Save** to save the changes.
13. Log in to the CLI, and execute the following commands:

```
% set system admin <system name> fips-140-2 mode enabled
% commit
```

NOTE: To ensure correct functioning and compliance with this Security Policy, module operators must use phones that support TLS v1.2.

Setting the module into FIPS mode will accomplish the following actions:

- All SSH keys will be regenerated.
- Encryption keys used by the system Configuration Database will be regenerated.
- All persistent CSPs stored on the system will be zeroized.

After completion and confirmation of the above steps, the system will reboot. After this reboot, and on all subsequent reboots, the module will be in its FIPS-Approved mode of operation.

3.1.4 Restoring Service to EMA

After FIPS mode is enabled, the CO must follow the procedures below to install new TLS certificates for EMA (running in Platform Manager mode) to be operational. This ensures that the keys to be used in FIPS mode are established while operating in FIPS mode. Importing of CA and SBC certificates is addressed in the “Restoring EMA in Platform Mode” section of the online document entry “[Enabling SBC for FIPS 140-2 Compliance](#)”.

3.1.4.1 Import New CA Certificate

To import new CA certificate, the CO must perform the following steps:

1. Import a new CA certificate by executing the following commands via the CLI:

```
> configure private
% set system security pki certificate caCert fileName caCert.der state enabled type
remote
% set profiles security EmaTlsProfile defaultEmaTlsProfile ClientCaCert caCert
% commit
```

3.1.4.2 Install New SBC Key and Certificate

The SBC’s TLS key and certificate can be generated externally or internally. To install an externally-generated SBC key and certificate, the CO must perform the following steps:

1. Transfer the PKCS #12-formatted key/certificate file to the SBC and save it as `/opt/sonus/external/<filename>.p12`.
2. Install the certificate by executing the following commands via the CLI:

```
> configure private
% set system security pki certificate sbxCert fileName sbxCert.p12 passphrase
<passphrase> state enabled type local
% set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName sbxCert
```

Alternatively, to install an locally-generated SBC key and certificate, the CO must perform the following steps:

1. Generate a certificate signing request (CSR) by executing the following commands via the CLI:

```
> configure private
% set system security pki certificate sbxCert type local-internal
% commit
% exit

> request system security pki certificate sbxCert generateCSR keySize keySize2K csrSub
"/C=US/ST=MA/L=Westford/O=Sonus Networks Inc./CN=www.sonusnet.com"
```

2. Copy the CSR output from the request in step #1 and obtain a signed certificate (in a PEM-formatted file) from an appropriate CA.
3. Transfer the certificate to the SBC and save it as `/opt/sonus/external/<filename>.pem`.
4. Install certificate by executing the following commands via the CLI:

```
> configure private
% set system security pki certificate sbxCert fileName sbxCert.pem
```

```
% set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName sbxCert
% commit
```

3.2 Crypto Officer Guidance

The Crypto Officer is responsible for initialization and security-relevant configuration and management of the module.

3.2.1 Management

Once installed, commissioned, and configured, the Crypto Officer is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to Section 3.1.3 for guidance that the Crypto Officer must follow for the module to be considered running in a FIPS-Approved mode of operation.

For additional information regarding the management of the module, please refer to the appropriate entries under Sonus' [SBC Core 6.2.x Documentation](#) webpage.

3.2.2 Default CO Password Use

The SBC 5400 supports multiple Crypto Officers. This role is assigned when the first CO logs into the system using the default username and password. The CO is required to change the default password as part of initial configuration. Only the CO can create other operators and configure the SBC module to operate in FIPS-Approved mode.

3.2.3 On-Demand Self-Tests

The power-up self-tests are automatically performed at power-up. The CO may initiate the power-up self-tests by issuing the reboot command or power-cycling the module.

Using the CLI, rebooting the module is accomplished using the following command:

```
% request system admin <systemName> restart
```

Using the EMA, rebooting the module is accomplished by navigating to **All -> System -> Admin -> <systemName> -> Admin Commands -> restart** on the SBC main screen.

Using the EMA in Platform Management Mode, rebooting the module is accomplished by navigating to **Administration -> System Administration -> Platform Management -> Reboot Platform** on the SBC main screen.

3.2.4 Zeroization

There are many CSPs within the module's cryptographic boundary including symmetric keys, private keys, public keys, and login passwords hashes. CSPs reside in multiple storage media including the SDRAM and system SSD. All ephemeral keys used by the module are zeroized on reboot, power cycle, or session termination. Keys and CSPs on the SSD of the module can be zeroized by using commands via EMA or CLI. The zeroization of the CDB Key

renders other keys and CSPs stored in the non-volatile memory of the CDB useless, effectively zeroizing them. The public key used for the firmware load test is stored in a file in the flash file system, and cannot be zeroized. Reinstallation of the firmware also erases all the volatile and non-volatile keys and CSPs from the module.

Using the CLI, keys and CSPs are zeroized using the following command:

```
% request system admin <systemName> zeroizePersistentKeys
```

Using the EMA, keys and CSPs are zeroized by navigating to **All -> System -> Admin -> <systemName> -> Admin Commands -> zeroizePersistentKeys** on the SBC main screen.

3.2.5 Status Monitoring

At any point in time, an authorized operator can access the module via the CLI or the EMA and determine the FIPS mode status of the module. FIPS mode status can be viewed by issuing the following command on the CLI:

```
% show configuration system admin <systemName> fips-140-2 mode
```

When running in Approved mode, the command will return the following message:

```
mode enabled
```

The FIPS mode status of the module can also be viewed using the EMA by navigating to **All -> System -> Admin -> Users and Application Management -> Fips 140-2** from the SBC main screen.

Once the module is properly configured, the Crypto Officer is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. The Crypto Officer shall monitor the module's status regularly. If any irregular activity is noticed, or the module is consistently reporting errors, customers should consult the online document entry "[SBC Troubleshooting Tools](#)" to resolve the issues. If the problems cannot be resolved through these resources, Sonus customer support should be contacted.

3.2.6 Firmware Upgrades

To upgrade the module's application firmware (including the ConnexIP OS and BIOS⁶¹ firmware), the CO shall complete the following procedure:

1. Download the SBC application package from the Salesforce customer portal to the local folder on a PC or remote server.
2. Validate the SBC md5 checksum using the checksum calculator.
3. Launch the EMA in Platform Management Mode.
4. Upload the desired SBC application package to SBC server using the **Upload Files** tab.
5. Stop the SBC application using **Admin -> Stop Application**. Confirm the stop operation with the CO credentials.
6. Navigate to **SW Install -> Upgrade SBC Application** tab. Select the **SBC Application Version** to upgrade and click **Next**.
7. Confirm the upgrade by providing CO credentials and click **Upgrade**. The upgrade process starts on the SBC and displays the upgrade status on **View Application Upgrade Log** screen.

⁶¹ BIOS – Basic Input/Output System

8. Launch the EMA and log on using the default credentials (change the password if logging for the first time).
9. Verify the SBC application status on the **Administration -> System Administration -> Platform Management** screen.
10. Verify the new OS and SBC application versions in **Monitoring->Dashboard->System and Software Info**.

For additional details regarding the module's firmware upgrade process, please refer to the Sonus Support online document entry "[Upgrading SBC Application in Standalone Configuration](#)".

3.3 User Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their password. The User must be diligent to pick strong passwords, and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret or private keys in their possession.

3.4 Additional Guidance and Usage Policies

This sections notes additional policies below that must be followed by module operators:

- As noted above, operator access to the BMC is provided over two external ports: an RS-232 serial port and a 1 Gbps Ethernet port (called the BMC Field Service Port). The CO must use these ports in order to accomplish the module's initial setup and configuration as described in section 3.1.1 above. Beyond this, the BMC's external ports shall not be used while the module is operational. Use of the BMC's external ports is prohibited while the module is operating in its FIPS-Approved mode. The CO shall ensure that operators do not directly access the module via the BMC's external ports for any purpose.
- Only the CO can create other operators.
- Password complexities can be configured by the Crypto Officer. All operators shall follow the complex password restrictions. The password may contain any combination of minimum eight letters (upper- and lower-case), numbers, and special characters allowing for a total of 95 possible characters. A password shall have:
 - Between 8 and 24 characters
 - At least one digit
 - At least one lower-case letter
 - At least one upper-case letter
 - At least one special character
- In the event that the module's power is lost and then restored, a new key for use with the AES GCM encryption shall be established.
- When using local certificate management mode, certificates are first stored in encrypted form on the external workstation prior to being sent to the module via SSH. The encryption key is established using PBKDF2 as specified in *NIST SP 800-132*. To ensure that the certificate file can be properly decrypted and installed once sent to the module, the encryption algorithm used on the external workstation must be 128-bit AES or 3-key Triple-DES in CBC mode, and the salt length used on the external workstation as input to the PBKDF2 must be 128 bits. Additionally, module operators will need to enter the same passphrase that was used on the external workstation in order to derive the appropriate decrypting key.

- The CO shall ensure that only RSA keys providing at least 112 bits of encryption strength are used for signing certificate requests.
- The module allows for the loading of new firmware, and employs an Approved message authentication technique to test its integrity. However, to maintain an Approved mode of operation, the CO must ensure that only FIPS-validated firmware is loaded. Any operation of the module after loading non-validated firmware constitutes a departure from this Security Policy.
- The EMA (running in Platform Manager mode) provides a checkbox that a module operator can use to continue with a firmware upgrade after a failed load test. The Crypto Officer shall ensure that the checkbox remains unchecked while the module is operating in its Approved mode. Any operation of the module after loading unverified firmware constitutes a departure from this Security Policy.
- To ensure that remote authentication is performed over a secured link, the CO shall set the authentication method to PEAP⁶²/MS-CHAPv2⁶³ when configuring the module for RADIUS authentication. For RADIUS authentication configuration guidance via the CLI and the EMA, please refer to the online document entries "[Radius Authentication - CLI](#)" and "[Radius Authentication – Radius Server](#)", respectively.
- The CO shall ensure that the module performs no more than 2^{16} encryptions with a given Triple-DES key.

3.5 Non-Approved Mode of Operation

When in the operational state, the module can alternate service-by-service between Approved and non-Approved modes of operation. The module will switch to the non-Approved mode upon execution of a non-Approved service. The module will switch back to the Approved mode upon execution of an Approved service.

3.5.1 Security Functions

The module includes the following non-Approved algorithm(s) that shall only be used in a non-Approved mode of operation:

- IKE v1/v2 KDF (non-compliant)

3.5.2 Roles

The module supports the Crypto Officer and User roles while in the non-Approved mode of operation.

3.5.3 Services

Table 11 below lists the service available in the non-Approved mode of operation.

⁶² PEAP – Protected Extensible Authentication Protocol

⁶³ MS-CHAPv2 – Microsoft Challenge-Handshake Protocol version 2

Table 11 – Non-Approved Service

Service	Operator		Description
	CO	User	
Establish IPsec Session (non-compliant)	✓	✓	Establish remote session using IPsec protocol

4. Acronyms

Table 12 provides definitions for the acronyms used in this document.

Table 12 – Acronyms

Acronym	Definition
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BIOS	Basic Input/Output System
ASCII	American Standard Code for Information Interchange
BMC	Baseboard Management Controller
CA	Certificate Authority
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CDR	Call Data Record
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DC	Direct Current
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
EC	Elliptical Curve

Acronym	Definition
ECC	Elliptical Curve Cryptography
ECDSA	Elliptical Curve Digital Signature Algorithm
EMA	Embedded Management Application
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENUM	E.164 NUmber Mapping
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HA	High Availability
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IKE v1	Internet Key Exchange version1
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Megabits per second
MD5	Message Digest 5
MKEK	Master Key Encrypting Key
MS-CHAPv2	Microsoft Challenge-Handshake Protocol version 2
N/A	Not Applicable
NAT	Network Address Translation
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NP	Network Processor
NTP	Network Time Protocol
OS	Operating System
PBKDF2	Password-Based Key Derivation Function 2

Acronym	Definition
PEAP	Protected Extensible Authentication Protocol
PKCS	Public-Key Cryptography Standards
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Riverst, Shamir, and Adleman
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-Factor Pluggable
SFTP	SSH (or Secure) File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Packet
USB	Universal Serial Bus
VOIP	Voice Over Internet Protocol

Prepared by:
Corsec Security, Inc.



13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
<http://www.corsec.com>

